SECURE SERVICE PROVISION FOR RELIABLE SERVER POOLING IN MANET

Giovanni Di Crescenzo
Security and Information Assurance Department
Telcordia Technologies Inc., Piscataway, New Jersey
Renwei Ge, Gonzalo R. Arce
Department of Electrical and Computer Engineering
University of Delaware, Newark, Delaware

ABSTRACT

The unique characteristics of battlefield mobile ad hoc networks bring severe security challenges to the application of reliable server pooling (rSerPool). This paper uses a novel threshold signature scheme with the features of ad hoc sever selection and dynamic group membership to secure the service provision phase of the rSerPool application in MANET. Our distributed and survivable threshold signature scheme can tolerate "single point of failure" and Byzantine attacks. Its ad hoc server selection increases service availability and decreases service latency. Our signature scheme provides essential authentication service in rSerPool and can be further used as part of distributed certificate authority in MANET.

I. INTRODUCTION

Mobile ad-hoc networks (MANETs) are of increasing interest for a diverse set of applications on the battlefield. Instead of using a centralized infrastructure, nodes in MANET cooperate with each other to provide networking during their movements. Such capability is essential for the Future Combat Systems on the battlefield where pre-existing or centralized communication infrastructures are not available. MANET on the battlefield can provide various services to support different missions, such as enemy situation, battlefield map, etc. Successful realization of these services confronts tremendous challenges not only from a harsh communication environment due to the factors of node mobility, radio fading and interfering, but also from enemies' attacks. Preserving the reliability of the services on the battlefield is as important as the services themselves.

Reliable server pooling (rSerPool) is an approach that provides the reliability of services by introducing redundancy in the number of servers available to a client. There are three classes of entities in the rSerPool architecture: Pool Element (PE), Name Server (NS) and Pool User (PU). PE is one of the servers that provide same service functionality. NS is responsible for maintaining server pools which includes pool name resolution, PE registration/deregistration, load balance and cooperation with other NSs. PU is the client being served by PEs. When one PE is dropped in the middle of service due to any of a number of possible reasons, the PU can still be served by the next available PE without breaking the current session. The architecture and protocols for the management and operation of rSerPool are being developed by IETF [1] to support highly reliability-demanding applications on Internet. The advantages of rSerPool, especially the failover merit, also make it very attractive in tactical mobile ad hoc networks.

The unique features of battlefield MANETs bring the application of rSerPool serious challenges in security. Wireless links are susceptible to attacks from passive eavesdropping to active impersonating. Nodes roaming in battlefield have non-negligible probability of being compromised. The compromised node would launch Byzantine attacks from the inside of the network. Trust relationships among nodes may change from time to time due the change of network topology and membership. Based on the analysis of security threats and requirements of rSerPool in MANET, we propose a novel ad-hoc threshold signature scheme as a basic cryptographic component to secure the service provision of rSerPool, especially to tolerate Byzantine attacks.

II. THRESHOLD SIGNATURES IN MANET

Threshold digital signature schemes with parameters (t, n) satisfy the following properties: at least $t + 1$ parties are able to generate a signature on a given message; at most t parties are not able to generate a valid signature; finally, any $t < n/2$ parties (where n is the total number of parties) cannot prevent the remaining honest parties to generate a threshold signature.

In the traditional threshold signature scheme, the threshold value t and the number of participants n are fixed after the protocol is initiated. Such fixed values do not match the rapid change of nodes' availability and connectivity in MANET. In our scheme, both t and n can be selected dynamically based on current network characteristics. Novelties of our ad-hoc threshold signature scheme include: ad hoc server selection and dynamic group member addition / deletion. The proposed scheme can be divided into two phases: (a) distributed key generation and (b) signature generation. We assume that secure routing is available in the former phase only. In the key generation phase, our scheme

Prepared through collaborative participation in the Communications and Networks Consortium sponsored by the U. S. Army Research Laboratory under the Collaborative Technology Alliance Program, Cooperative Agreement DAAD19-01-2-0011.

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **00 DEC 2004**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE **Secure Service Provision For Reliable Server Pooling In Manet**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Security and Information Assurance Department Telcordia Technologies Inc., Piscataway, New Jersey; Department of Electrical and Computer Engineering University of Delaware, Newark, Delaware**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM001736, Proceedings for the Army Science Conference (24th) Held on 29 November - 2 December 2005 in Orlando, Florida. , The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**2**	

is similar to [2], but with two major differences. First, each party randomly chooses different sets of secrets and corresponding polynomials for different threshold values; assume there are up to τ compromised servers, then $t \in \{\tau, \ldots, \lfloor n/2 \rfloor\}$. Second, the public key of threshold signature is not determined at the end of the phase, but different public keys for different threshold values and different desired subset of parties are implicitly defined. In the signature generation phase, a client selects a subgroup of servers based on the network's present characteristics and sends his selection and the threshold value to the chosen servers. Each selected server then uses these values in the generation of a bandwidth and computation efficient partial signature with a careful modification of the algorithm in [3]. The detailed protocols of proposed ad hoc threshold signature and cryptographic proof can be found in our paper [4].

Our simulation also shows the advantage of the proposed scheme. The simulation compares two scenarios: one is with the group of servers fixed at the beginning; the other is with the ad hoc group of dynamic server selection. The simulation is carried on the simulator QUALNET. The detail settings are the following: 30 nodes randomly placed in a 1500m × 1500m flat plane; Random way point with speed [2,20] m/s and 30 sec pause; IEEE802.11 physical layer and MAC layer; AODV routing protocol. The chosen threshold is $(2, 5)$. There are two timeouts in the client side to limit severe delay: request-transmitting timeout and response-waiting timeout. CBR(Constant Bit Rate) flows are used to simulate the network traffic. Fig. 1 shows the average success rate of obtaining valid signatures. With the increasing of the CBR bit rate, the traffic in MANET becomes more and more intense and clients experience longer and longer delay. Frequent timeouts make all the curves decrease. But it is clear to see that the success rate of threshold signatures with ad hoc server selection is much better than the case of fixed servers.

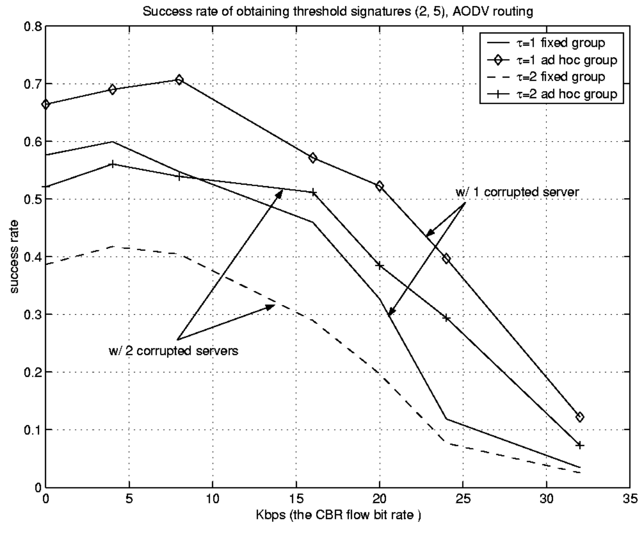

Fig. 1. The rate of obtaining valid signatures successfully

III. SECURE SERVICE OF RSERPOOL

Threshold signature provides essential authentication service in rSerPool. After NSs finish key agreement phase, each PE registers its service to the NSs. Instead of contacting one NS, a PE contacts several NSs. After providing NSs the proof of the service it claims, PE then asks for the registration and the threshold signature on its public key, i.e., certificate. Name resolution is the step that PU asks NS to provide a list of addresses of available PEs providing certain service. Similar to PE registration, a PU contacts several NSs to get the resolution signed by each of the chosen NSs. NSs can also provide the threshold signature on PU's public key. With the certificates provided by NSs, PE and PU can authenticate each other and build a private channel for further communication. NSs can also keep a revocation list in their database for query. In other words, the NSs can play the role of distributed certificate authority in MANET, thus avoiding problems with ordinary CA's such as "single point of failure" and allowing a Byzantine adversary to corrupt a small number of NSs. Note that, although NSs are the major entities to issue threshold signatures, PE and PU can also join the protocols and provide threshold signatures. Therefore, reliable service provided between PEs and PUs can be resistant with respect to failover of a small number of PEs, and even tolerates corruption of a small number of PEs by a Byzantine adversary. We stress that our constructions of a distributed certificate authority in MANET and of a secure rSerPool are based on essentially minimal model assumptions (a threshold bound on the number of failovers or nodes corrupted by an adversary, and availability of secure routing only required in a preliminary phase, run only once).

IV. CONCLUSION

A novel threshold signature scheme with the features of ad hoc sever selection and dynamic membership is presented in the paper to secure the service provision of rSerPool in MANET, and especially to tolerate the Byzantine attack. We note that our threshold scheme and analysis can be applied to secure other applications in MANET.

The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government.

V. REFERENCES

[1] "Architecture for reliable server pooling," *draft-ietf-rserpool-arch-01.txt, work in progress.*

[2] T. Pedersen, "A threshold cryptosystem without a trusted party," Proceedings of Eurocrypt 1991.

[3] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," Proceedings of Asiacrypt 2001.

[4] G. Di Crescenzo, G. R. Arce, and R. Ge, "Threshold cryptography for mobile ad hoc networks," Proc. of Security in Communication Networks '04, Amalfi, Italy.